



## Setting Up Event Logs

---

Use the Logs menu to set up and view event logs on the bridge.

Here's what you'll find in this chapter:

- [Event Logs, page 10-2](#)
- [Using the Logs Menu, page 10-3](#)
- [Severe Error Log, page 10-3](#)

# Event Logs

The bridge produces logs that record significant events occurring within your bridge and on the infrastructure. The type of logs include the following:

- **Information log:** records status changes that occur in the normal operation of the system. For example, when an end node associates to a parent access point.
- **Error log:** records errors that occur occasionally, but which are easily recovered from by the bridge. For example, errors that occur during the reception and transmission of packets to and from the bridge.
- **Severe error log:** records errors that drastically affect the operation of the system. The system continues to run, but action is required to return the bridge to normal operating standards.

## Information Log

The following events appear in the Information log:

- **BOOTP/DHCP set new IP address:** the BOOTP/DHCP server answered the request and assigned the bridge an IP address different from the configured value.
- **Node “node address” “device name” added:** a nonvolatile entry was added to the association table.
- **Node “node address” “device name” “ASCII name” removed, max radio retries:** a node was removed from the table because a response was not received from the node after attempts were made to transmit a packet to it. The node may have failed or moved to another cell.
- **RARP set new IP address:** a Reverse Address Resolution Protocol (RARP) server answered a request for an IP address with an address different from the one currently saved. The currently saved value is overwritten.
- **Connected to parent “node address”:** The bridge associated to its parent node.
- **SNMP: “command text”:** a SNMP management station sent the bridge a *set* variable request which was successfully executed. The *command text* is a similar menu command that has the same effect as the SNMP request.
- **SNMP access failure from “community name” “IP address” (node address):** a SNMP management station attempted to access the SNMP agent with an invalid community name or a name that it was not allowed to use.
- **TFTP is loading “file name” from “ip address”:** the BOOTP server gives the bridge the name of a configuration file and then the name of a firmware file to load.
- **Node “node address” Enode removed, staled out:** a wired Ethernet node was removed from the MAC address table due to lack of activity, based upon the setting of the `_Staletime_option`.

## Error Log

The following events appear in the Error log:

- **“Category” Error: nnn “type” errors:** an error occurred that is marked by an asterisk \* after its count in the statistics displays. These errors are serious enough to affect the operation of the bridge. See the sections on each display for an explanation of each error.

- **Unable to locate IP address “ip address”**: the bridge was trying to send a packet to an IP address without knowing the hardware node ID. When this occurs, the bridge uses the ARP protocol to try to determine the proper address. This event is logged if there was no answer to the ARP request. Usually the bridge is trying to find the destination for the SNMP traps.

## Severe Error Log

The following events appear in the Severe Error log.

- **Ethernet cabling problem**: if no traffic was sent or received on the Ethernet cable in the last 10 seconds, the bridge sends a packet to itself to test the connection. If the transmission succeeds, the timer is reset. If it fails, this event is logged and traffic for the connection is discarded until the test succeeds.
- **Configuration is too large to save**: the number of commands in the configuration is too large for the available nonvolatile memory. This error might be caused by too many nonvolatile entries in the association table.
- **Could not program the flash memory**: an error occurred when trying to program a new version of the firmware into flash memory. The bridge must be serviced.
- **Lost our association, max radio retries**: the bridge lost communications with its parent node after trying to send a packet the maximum number of times. The bridge will try to re-associate. The problem may be a parent access point failure. All local associations will be dropped.
- **Lost our association, radio restarted**: a radio configuration parameter was changed. All associations are dropped and the radio is restarted.
- **Lost our association, new specified router**: the specified router parameter of this bridge was changed. The bridge drops its current association and tries to reassociate.
- **Lost our association, NAK from router**: the bridge responds as though it was associated to its parent but the parent does not have the association. The bridge will attempt to reassociate. The parent may have been rebooted.
- **The address PROM is invalid**: each bridge contains a programmable read-only memory (PROM) chip that contains the bridge’s hardware address. During power up, the bridge was not able to read a valid address from the PROM. The bridge must be serviced.

## Using the Logs Menu

Use the Logs menu to view event logs.

**Console:** Choose **Main > Logs**

**Browser:** Click **Logs**

Table 10-1 lists the Logs menu options and parameters.

Table 10-1 Logs Menu Options and Parameters

Option	Description										
Log alarm history (History)	<p>Displays a history of the events that have occurred on the bridge and the infrastructure.</p> <p>All events are stored within the bridge in a 10-KB memory buffer. The actual number of events the bridge saves depends on the size of each log stored in the buffer.</p> <p>Log events display in a least-recent to most-recent order. If the memory buffer becomes full, the oldest event in the buffer is replaced by the most recent.</p> <p>Only events that occurred since the bridge was last powered up or since the memory buffer was cleared are saved.</p> <p>If a power failure occurs, events contained in the memory are not saved.</p> <p>The display looks similar to the following.</p> <pre> OLDEST 0:00:00 I Node 004096109e30 APBR2000-E Floor_2_109e30 added locally 0:00:03 I Node 0040961064de AP2000-E F3_1064de added for 004096109e30 30:35:09 NEWEST, cleared at 0:00:00 b[ackward], f[orward], n[ewest], o[ldest], a[ll], C[lear], q[uit] </pre>										
	<table border="1"> <thead> <tr> <th>Display line</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>First line</td> <td><i>OLDEST</i> indicates the end of the buffer display. This word appears at the end of the history log.</td> </tr> <tr> <td>Display lines</td> <td>Display the time since power-up that the event occurred, the severity level (I=information, E=error, S=severe) and the actual event text.</td> </tr> <tr> <td>Last line</td> <td>Indicates the current time and the time the buffer was last cleared by the operator. <i>NEWEST</i> indicates the start of the history log.</td> </tr> <tr> <td>Option line</td> <td>Indicates the movement keys to use when viewing the history log. Since displaying the entire history uses more than a screen page, use the keys to navigate through the history log.</td> </tr> </tbody> </table>	Display line	Description	First line	<i>OLDEST</i> indicates the end of the buffer display. This word appears at the end of the history log.	Display lines	Display the time since power-up that the event occurred, the severity level (I=information, E=error, S=severe) and the actual event text.	Last line	Indicates the current time and the time the buffer was last cleared by the operator. <i>NEWEST</i> indicates the start of the history log.	Option line	Indicates the movement keys to use when viewing the history log. Since displaying the entire history uses more than a screen page, use the keys to navigate through the history log.
Display line	Description										
First line	<i>OLDEST</i> indicates the end of the buffer display. This word appears at the end of the history log.										
Display lines	Display the time since power-up that the event occurred, the severity level (I=information, E=error, S=severe) and the actual event text.										
Last line	Indicates the current time and the time the buffer was last cleared by the operator. <i>NEWEST</i> indicates the start of the history log.										
Option line	Indicates the movement keys to use when viewing the history log. Since displaying the entire history uses more than a screen page, use the keys to navigate through the history log.										
Clear the history buffer (Clear)	Deletes all event entries from the history buffer.										

**Table 10-1** Logs Menu Options and Parameters

Option	Description										
Type of log to print (Printlevel)	Specifies the type of event logs that appear on the console screen. The level you select determines which events or errors appear on the screen. <b>Default:</b> Severe <b>Range:</b> Error/severe, severe, all										
	<table border="1"> <thead> <tr> <th>Log Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Error/severe</td> <td>Displays all errors and severe errors.</td> </tr> <tr> <td>Severe</td> <td>Displays severe errors only.</td> </tr> <tr> <td>All</td> <td>Displays all errors, severe errors and information.</td> </tr> </tbody> </table>	Log Type	Description	Error/severe	Displays all errors and severe errors.	Severe	Displays severe errors only.	All	Displays all errors, severe errors and information.		
	Log Type	Description									
	Error/severe	Displays all errors and severe errors.									
	Severe	Displays severe errors only.									
All	Displays all errors, severe errors and information.										
Type of logs to save (Loglevel)	Specifies the type of log you want to save to memory and view on the history log screen. <b>Default:</b> All <b>Range:</b> Error/severe, severe, all										
	<table border="1"> <thead> <tr> <th>Log Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Error/severe</td> <td>Displays all errors and severe errors.</td> </tr> <tr> <td>Severe</td> <td>Displays severe errors only.</td> </tr> <tr> <td>All</td> <td>Displays all errors, severe errors and information.</td> </tr> </tbody> </table>	Log Type	Description	Error/severe	Displays all errors and severe errors.	Severe	Displays severe errors only.	All	Displays all errors, severe errors and information.		
	Log Type	Description									
	Error/severe	Displays all errors and severe errors.									
	Severe	Displays severe errors only.									
All	Displays all errors, severe errors and information.										
Type of logs to light status LED (Ledlevel)	Triggers the indicator status LED to turn amber when a specific type of event or error occurs. <b>Default:</b> Error/severe <b>Range:</b> Error/severe, severe, all, off										
	<table border="1"> <thead> <tr> <th>Event</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Error/severe</td> <td>Displays all errors and severe errors.</td> </tr> <tr> <td>Severe</td> <td>Displays severe errors only.</td> </tr> <tr> <td>All</td> <td>Displays all errors, severe errors and information.</td> </tr> <tr> <td>Off</td> <td>No events are displayed</td> </tr> </tbody> </table>	Event	Description	Error/severe	Displays all errors and severe errors.	Severe	Displays severe errors only.	All	Displays all errors, severe errors and information.	Off	No events are displayed
	Event	Description									
	Error/severe	Displays all errors and severe errors.									
	Severe	Displays severe errors only.									
	All	Displays all errors, severe errors and information.									
Off	No events are displayed										
Set alarm on statistics (Statistics)	Controls how alarms are generated based on any of the available statistics kept by the bridge. Logs may be: <ul style="list-style-type: none"> <li>• Disabled for statistics</li> <li>• Generated if the statistic changes at all</li> <li>• Generated if the statistic changes at a greater than specified rate</li> </ul> <b>Note</b> See the section “Setting Statistic Parameters” later in this chapter.										

**Table 10-1** Logs Menu Options and Parameters

Option	Description
Log network roaming (Network)	<p>If enabled, logs any change to radio nodes in the network.</p> <p><b>Default:</b>Off</p> <p><b>Range:</b> On or off</p> <p>Normally, the bridge only logs changes in location for a client that moves to or from this unit.</p>
Log backbone node changes (Bnolog)	<p>If enabled, logs clients that roamed to different backbone nodes.</p> <p><b>Default:</b>Off</p> <p><b>Range:</b> On or off</p> <p>Normally, the bridge only logs changes in the state or location of its own radio nodes.</p>
IP destination for SNMP traps (Trapdest)	<p>Displays a menu of SNMP trap actions.</p> <p>Generates SNMP trap messages to a particular Network Management Station (NMS) whenever a significant event occurs.</p> <p>With SNMP enabled and the <i>Trapdest</i> option configured with a valid IP address, the system generates SNMP trap messages. If the <i>Trapdest</i> option is set to <i>none</i> or if the IP address 0.0.0.0 is typed, traps are not sent.</p> <p>The following trap messages are sent as they occur:</p> <ul style="list-style-type: none"> <li>• A cold start trap is sent when the bridge first powers up.</li> <li>• A link up trap is sent when the configuration is changed or restored for a severe error condition.</li> <li>• A link down trap is sent when the configuration is changed or encounters a severe error condition.</li> <li>• A link up trap is sent for a bridge as soon as the radio is configured.</li> <li>• An authentication failure trap is sent if an SNMP request is received with an unknown community name. You can disable this trap by setting the <i>Authtrap</i> parameter to <i>off</i>. See “Logging Failed Attempts (<i>Authtrap</i>)” later in this chapter.</li> <li>• Any normal alarms and logs you have configured to be sent by setting the <i>Loglevel</i> parameter.</li> </ul> <p>Since the path to the trap destination may be through a failed or not yet established radio link, it is possible that cold start and link down traps could be lost.</p>
Community for SNMP traps (Trapcomm)	Specifies the community name to be used in the trap message.

**Table 10-1** Logs Menu Options and Parameters

Option	Description
Type of log to cause a trap (Loglevel)	<p>Enables the bridge to generate an enterprise specific trap whenever an event of a given severity or higher is recorded.</p> <p><b>Note</b> The <i>Trapdest</i> option must be set to <i>on</i>.</p> <p>The generated trap contains the text of the event message along with the severity of the event. The different severities are:</p> <ul style="list-style-type: none"> <li>• <b>Error/severe:</b> displays all errors and severe errors.</li> <li>• <b>Severe:</b> displays severe errors only.</li> <li>• <b>All:</b> displays all errors, severe errors and information.</li> <li>• <b>Off:</b> no events are displayed.</li> </ul>
Enable authorization failure trap (Authtrap)	<p>Allows logging of failed attempts of SNMP authentication.</p> <p><b>Default:</b> Off</p> <p><b>Range:</b> On or off</p> <p>Default setting is <i>off</i> which means authentication failures are not logged.</p>
UNIX syslog address (Syslog)	<p>The <i>Syslog</i> option forwards events to a UNIX host running the <i>Syslogd daemon</i> process. Enter the IP address of the UNIX host. If the address remains at the default of 0.0.0.0, events are not sent. You can control the type of events sent to the daemon with the <i>Syslevel</i> option, which has the same arguments as the <i>Printlevel</i> function.</p>
Type of log to send to syslog (Syslevel)	<p>Packets received by the Syslogd daemon process are recorded in the system log file on the UNIX host. The events display on the console and are forwarded to the UNIX host. If the bridge should fail for any reason, the events can still be viewed on the UNIX host.</p>
Syslog facility to send (Facility)	<p>The events carry the syslog facility code <i>LOG_LOCAL0</i>, which has a value of 16. You can change this value with the option <i>Facility</i>. The syslog priority depends on the priority of the events locally.</p>
Enable reception of syslog messages (Rcvsyslog)	<p>On the UNIX host, the <b>Syslogd</b> daemon process usually adds the current time and IP address of the bridge that sent the event. The bridge pre-pends its own name to the event before it is sent. See the following example.</p> <pre>Jan 11 10:46:30 192.009.200.206 AIR-WGB340_285e73: Node 0000c0d1587e ENODE added for 004096285e73</pre> <p>By default, the bridge receives and displays syslog messages from other bridges in the network. The <i>Rcvsyslog</i> option enables or disables this function. You could choose one bridge to monitor and have all other units configured with this bridge as their syslog host.</p>

## Setting Statistic Parameters

To set statistic parameters, follow these steps:

**Step 1** Select **Statistics**.

**Step 2** The following menu appears:

```

1. ra Radio
2. re Radio Error
3. et Ethernet
4. ee Ethernet Error

Enter category, one of [a number from 1 to 4, a short form]
: █

```

44805

Enter your statistics category choice. Enter the number or the short form. The short form is used to store the command in the configuration.

**Step 3** The menu of the types of statistics for your chosen statistics category appears. For example, if you enter **1\_ra Radio**, the following menu appears:

```

                Radio
    Receive                Transmit
1 rpa Packets             5 tpa Packets
2 rby Bytes               6 tmu Multicasts
3 rfi Filtered           7 tby Bytes
4 rer Errors              8 ter Errors

Enter one of [a index from 1 to 8, a short form] : █

```

44804

**Step 4** If any of the statistics already have an alarm associated, the current setting is displayed after the name.

Enter a category number or the short form of the particular statistics that you wish to change and press **Enter**. The following prompt appears:

Enter an action, one of [off, any, rate]:

**Step 5** Choose an action from the following list:

- **Off:** turns off any alarms based on the statistics value.
- **Any:** generates an alarm if the statistics change value.
- **Rate:** prompts for a rate-per-second change. If the statistic value changes faster than this rate, an alarm is produced.